National Infrastructure Protection Center CyberNotes

Issue #2002-08 *April 22, 2002*

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between April 4 and April 18, 2002. The table provides the vendor, operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear in italicized colored text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Allaire[1]	Windows 95/98/NT 4.0/2000, Unix	ColdFusion Server 4.0, 4.5, 5.0	A vulnerability exists when a web request is made for a certain non-existent .cfm or .dbm file, which could let a remote malicious user obtain sensitive information.	The vendor suggests turning on "Check that file exists" Windows 2000: Open the Management console; Click on "Internet Information Services"; Right-click on the website and select "Properties"; Select "Home Directory"; Click on "Configuration"; Select ".cfm"; Click on "Edit"; Make sure "Check that file exists" is checked; and Do the same for ".dbm"	ColdFusion DOS Device File Request System Sensitive Information	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[1] KPMG-2002013, April 18, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
America OnLine[2]	Windows 98/ME/NT 4.0/2000, MacOS X 10.x, Unix	AOLServer 3.0, 3.2 Win32, 3.2 Unix, 3.3 Win32, 3.3.1, 3.4 Win32, 3.4, 3.4.2 Win32, 3.4.2,	A format string vulnerability exists in the in the 'Ns_PdLog' function of the library, which could let a malicious user execute arbitrary code and obtain elevated privileges.	AOLServer has been patched.	AOLServer Ns_PdLog() Format String	**High**	Bug discussed in newsgroups and websites.
America OnLine[3]	Windows 95/98/ME/ NT 4.0/2000	Instant Messenger 4.0-4.7	A vulnerability exists in the 'Direct Connection' feature due to the way embedded objects are handled during direct connections with other users, which could let a malicious user create arbitrary files.	No workaround or patch available at time of publishing.	AOL Instant Messenger Arbitrary File Creation	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Anthill[4]	Multiple	Anthill 0.1.6.1 & prior	Two vulnerabilities exist: a vulnerability exists in the 'postbug.php' component because no authentication is required, which could let a remote malicious user bypass the 'enterbug.php' authorization; and a vulnerability exists because user input is not properly sanitized, which could let a malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	Anthill Multiple Vulnerabilities	Medium/ **High** **(High if arbitrary script code can be executed)**	Bug discussed in newsgroups and websites.
Aprelium Technol-ogies[5]	Windows 95/98/ME/ NT 4.0/2000, XP	Abyss Web Server 1.0	Several vulnerabilities exist: a vulnerability exists when a specially crafted web request containing encoded sequences is sent to the server, which could let a remote malicious user obtain access to the administrative configuration files; and a vulnerability exists because the administrative password is stored in plaintext, which could let a remote malicious user obtain administrative access.	Patch available at: http://www26.brinkster.com/netcrash/abyssws.zip	Abyss Web Server Administrative Access	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
ASP-Nuke[6]	Multiple	ASP-Nuke RC1	A vulnerability exists because script code is not adequately filtered from image tags, which could let a malicious user execute arbitrary script code.	Upgrade available at: http://www.asp-nuke.com/	ASP-Nuke Image Tag	**High**	Bug discussed in newsgroups and websites.

[2] INTEXXIA(c) Security Advisory, 1052-300102, April 16, 2002.
[3] Bugtraq, April 16, 2002.
[4] Bugtraq, April 6, 2002.
[5] Bugtraq, April 10, 2002.
[6] SecurityFocus, April 10, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
ASP-Nuke[7]	Multiple	ASP-Nuke RC1, RC2	Several Cross-Site Scripting vulnerabilities exist because user-supplied input in not properly stripped of commands when the 'downloads.asp' and 'post.asp' pages build HTML content, which could let a malicious user execute arbitrary script code; a vulnerability exists because user issued cookies are stored in an unencrypted format, which could let a malicious user manipulate values in their cookie and authenticate as an arbitrary user of the service, including the administrative account; and a vulnerability exists because authentication cookies may be modified, which could let a malicious user obtain sensitive information.	Upgrade to ASP-Nuke RC3.	ASP-Nuke Cross-Site Multiple Vulnerabilities	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. There is no exploit code required for the plaintext cookie vulnerability.
Bradford Barrett[8]	MacOS X 10.0, Unix	Webalizer 2.0.1 –09, 2.0.1 -06	A buffer overflow vulnerability exists in the reverse resolving code if reverse DNS lookups are enabled, which could let a remote malicious user obtain root access.	As a workaround, reverse DNS lookup may be disabled until a fix is made available.	Webalizer Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Caldera International, Inc.[9]	Unix	OpenUnix 8.0; UnixWare 7.1.1	A buffer overflow vulnerability exists in the X11 library due to improper bounds checking when the 'xrm' flag is used, which could let a malicious user execute arbitrary code.	Patch available at: ftp://stage.caldera.com/pub/security/openunix/CSSA-2002-SCO.15	Caldera X11 Library -xrm Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
CGI SCRIPT. NET[10]	Unix	CSGuest book 1.0, CSLive Support 1.0, CSNews Professional 1.0, CSChat-R-Box 1.0	A Remote Code Execution vulnerability exists in the 'setup.cgi' file, which could let a remote malicious user execute arbitrary code.	Updates available at: http://www.cgiscript.net/	CS Guestbook Remote Command Execution	**High**	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Cisco Systems[11]	Multiple	AP340, AP350, BR350	A Denial of Service vulnerability exists if Telnet access is enabled and a password is required for authorization.	Upgrade available at: http://www.cisco.com	Cisco Aironet Telnet Authentication Denial of Service	Low	Bug discussed in newsgroups and websites.

[7] SecurityFocus, April 10, 2002.
[8] Securiteam, April 16, 2002.
[9] Caldera International, Inc. Security Advisory, CSSA-2002-SCO.15, April 11, 2002.
[10] Bugtraq, April 8, 2002.
[11] Cisco Security Advisory, 200204009, April 9, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Compaq Computer Corporation[12]	Unix	Tru64 4.0 g PK3 (BL17), Tru64 4.0 f PK7 (BL18), Tru64 5.0 a PK3 (BL17), Tru64 5.0, Tru64 5.1 a PK1 (BL1), Tru64 5.1 PK4 (BL18), Tru64 5.1	A buffer overflow vulnerability exists due to the way the 'LANG' and 'LOCPATH' environment variables are handled, which could let a malicious user obtain elevated privileges.	Patch available at: http://ftp1.support.compaq.com/public/unix/	Compaq Tru64 C Library Buffer Overflow	Medium	Bug discussed in newsgroups and websites.
Computer Associates[13]	Unix	CA-MLink	Buffer overflow vulnerabilities exist in the MLClear, MLLink, and MLLock programs due to inadequate bounds checking, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	CA-MLink Buffer Overflows	**High**	Bug discussed in newsgroups and websites.
Demarc Security[14]	Windows NT 4.0/2000, XP, Unix	PureSecure 1.0.5 Windows, 1.0.5 Unix	A vulnerability exists because a malicious user can bypass login authentication and obtain Administrative access by SQL injection through cookies.	Upgrade to 1.6 available at: http://www.demarc.com/downloads/puresecure/	PureSecure Authentication Bypass	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
EMUMail, Inc.[15]	Unix	EMUMail 3.0; EMUMail for Red Hat Linux 5.0, 5.1; EMUMail for Unix 5.1	A vulnerability exists in the 'type=' function of the 'emumail.cgi,' which could let a remote malicious user obtain sensitive information.	Upgrade available at: http://www.emumail.com/bin/EmuWebmail-5.1.0-PATCH101.tgz	EMUMail Arbitrary File Reading	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
EMUMail, Inc.[16]	Unix	EMUMail 3.0; EMUMail for Red Hat Linux 5.0, 5.1; EMUMail for Unix 5.0, 5.1	A vulnerability exists when a malicious HTTP Host value is supplied, which could let a malicious user execute arbitrary programs.	No workaround or patch available at time of publishing.	EMUMail HTTP Host Arbitrary Config File Loading	**High**	Bug discussed in newsgroups and websites.
FreeBSD[17]	Unix	FreeBSD 4.5 –STABLE, 4.5 - RELEASE	Multiple Denial of Service vulnerabilities exist in the SYN cache (syncache) and SYN cookies (syncookies) mechanism features.	Patch available at: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-02:20/syncache.patch	FreeBSD 4.5 syncache / syncookies Denial of Service	Low	Bug discussed in newsgroups and websites.

[12] Compaq Security Advisory, SSRT-541, April 18, 2002.
[13] Bugtraq, April 5, 2002.
[14] Demarc Security Update Advisory, April 16, 2002.
[15] Securiteam, April 6, 2002.
[16] Bugtraq, April 10, 2002.
[17] FreeBSD Security Advisory, FreeBSD-SA-02:20, April 16, 2002.

Vendor	**Operating System**	**Software Name**	**Vulnerability/ Impact**	**Patches/Workarounds/ Alerts**	**Common Name**	**Risk***	**Attacks/ Scripts**
FreeBSD[18]	Unix	FreeBSD 4.5 –STABLE, 4.5 - RELEASE	A Denial of Service vulnerability exists when an ICMP echo reply is sent because the number referencing the amount of hosts with current connections via that route is never decremented after termination of the ICMP traffic.	Patch available at: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-02:21/tcpip.patch	FreeBSD \ ICMP Echo Reply Denial of Service	Low	Bug discussed in newsgroups and websites.
Hewlett Packard Systems[19]	Mac OS X	Photosmart Print Driver for Mac OS X 1.2.1	A vulnerability exists in the world writable file, 'hp_imaging_connectivity,' which could let a malicious user replace the file with a Trojaned copy or compromise root.	No workaround or patch available at time of publishing.	Photosmart Mac OS X Print Driver Weak File Permissions	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Horde Project[20]	Unix	IMP 2.2.7	Two vulnerabilities exist: a Cross-Site Scripting vulnerability exist in the 'status.php3' component due to improper filtering of HTML and script code, which could let a malicious user execute arbitrary script code; and a path disclosure vulnerability exists in several of the scripts, which could let a malicious user obtain sensitive information.	Upgrade available at: ftp://ftp.horde.org/pub/imp/tarballs/imp-2.2.8.tar.gz Patch available at: ftp://ftp.horde.org/pub/imp/tarballs/patch-imp-2.2.7-2.2.8.gz	IMP Cross-Site Scripting & Path Disclosure	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
IBM[21]	Multiple	Informix Web Datablade 4.10-4.12	A vulnerability exists because SQL commands can be inserted into any page request, which could let a malicious user obtain sensitive information or elevated privileges.	No workaround or patch available at time of publishing.	IBM Informix Web Datablade Page Request SQL Injection	Medium	Bug discussed in newsgroups and websites. Several exploits have been published.
IBM[22]	Multiple	Informix Web Datablade 4.10-4.13	A vulnerability exists if HTML encoding is used to sanitize user input, which could let a malicious user execute arbitrary SQL code.	No workaround or patch available at time of publishing.	Informix Web Datablade SQL Query HTML Decoding	**High**	Bug discussed in newsgroups and websites. There is no exploit code required. Vulnerability has appeared in the press and other public media.
IBM[23]	Multiple	Tivoli Storage Manager 4.2, 4.2.1	A buffer overflow vulnerability exists when an unusually long username is supplied to the HTTP port, which could let a malicious user execute arbitrary code.	Upgrade available at: ftp://ftp.software.ibm.com/storage/tivoli-storage-management/patches/server/	Tivoli Storage Manager Buffer Overflow	**High**	Bug discussed in newsgroups and websites.

[18] FreeBSD Security Advisory, FreeBSD-SA-02:21, April 17, 2002.
[19] Bugtraq, April 15, 2002.
[20] SecurityFocus, April 7, 2002.
[21] Bugtraq, April 11, 2002.
[22] Bugtraq, April 11, 2002.
[23] iXsecurity Security Vulnerability Report, 20020328, April 11, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
IBM[24]	Windows NT 4.0/2000	Tivoli Storage Manager 4.2, 4.2.1	A buffer overflow vulnerability exists because adequate bounds checking is not performed by the TSM Client Acceptor, which could let a malicious user execute arbitrary code.	Contact IBM support for further information on obtaining the fix.	Tivoli Storage Manager Client Acceptor Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Internet Software Consortium[25]	Unix	INN 2.0-2.2.3	Multiple vulnerabilities exist in the 'inews' and 'rnews' components due to format string format string coding and insecure open() calls, which could let a malicious user obtain elevated privileges or the execute arbitrary code.	No workaround or patch available at time of publishing.	InterNetNews Multiple Vulnerabilities	Medium/ High **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Exploit script has been published.
LogWatch[26] ***RedHat issues update[27]***	**Unix**	**LogWatch 2.1.1**	**A vulnerability exists due to a race condition during the temporary directory creation, which could let a malicious user obtain unauthorized root access.**	**No workaround or patch available at time of publishing.** **Update available at:** ftp://updates.redhat.com/	**LogWatch Root Compromise**	**High**	**Bug discussed in newsgroups and websites. Exploit script has been published.**
Melange[28]	Multiple	Melange Chat System 2.0.2 Beta 2	Multiple buffer overflow vulnerabilities exist: an overflow exists when an unusually long line is included in the configuration file, one exists if the configuration file is renamed with an unusually long filename, and when an unusually large /yell argument that contains arbitrary data is submitted, which could let a remote malicious obtain sensitive information.	No workaround or patch available at time of publishing.	Melange Chat Systems Multiple Buffer Overflows	Medium	Bug discussed in newsgroups and websites.
MHonArc[29]	Multiple	MHonArc 2.5, 2.5.1, 2.5.2	A vulnerability because scripting tags are not properly filtered, which could let a malicious user execute arbitrary script code.	Update available at: http://www.mhonarc.org/tar/MHonArc2.5.3.tar.gz	MHonArc HTML Script Filter Bypass	**High**	Bug discussed in newsgroups and websites. Exploits have been published.
Microsoft[30]	Windows NT 4.0	BackOffice 4.0, 4.5	A vulnerability exists when an HTTP request is submitted directly to the 'services.asp,' which could let an unauthorized malicious user bypass the logon page.	Patch available at: http://download.microsoft.com/download/bofficesrv45/Update/4.x/NT4/EN-US/Q316838i.exe	BackOffice Server Web Administration Login Bypass	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[24] iXsecurity Security Vulnerability Report, 20020327, April 11, 2002.
[25] Bugtraq, April 11, 2002.
[26] Bugtraq, March 27, 2002.
[27] Red Hat Security Advisory, RHSA-2002:054-09, April 4, 2002.
[28] Bugtraq, April 14, 2002.
[29] Bugtraq, April 18, 2002.
[30] NGSSoftware Insight Security Research Advisory, NISR17042002A, April 17, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[31]	Windows 2000	IIS 5.0	A vulnerability exists in the in 'CodeBrws.asp' file, which could let a remote malicious user obtain sensitive information.	Unofficial workaround (Bugtraq): Remove the CodeBrws.asp script.	IIS CodeBrws. ASP File Extension Sensitive Information	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Microsoft[32]	Windows 95/98/ME/ NT 4.0/2000	Internet Explorer 5.0, 5.0.1, 5.0.1SP1&2, 5.5, 6.0; Outlook 2000, 2002; Outlook Express 4.0, 5.0, 5.5, 6.0; Word 2000, 2000 SR1, SP1a, SR2, 2002	A Denial of Service vulnerability exists if a malicious user creates an excessive number of VBScript ActiveX Word objects.	No workaround or patch available at time of publishing.	Microsoft VBScript ActiveX Word Object Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft[33]	Windows 95/98/ME/ NT 4.0/2000	Internet Explorer 5.0, 5.5, 5.5SP1&2, 6.0	A vulnerability exists in the 'dialogArguments' property because validation code only checks the original URL instead of the final URL, which could let al malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	Internet Explorer Dialog Origin Policy Bypass	High	Bug discussed in newsgroups and websites. Proof of concept exploits have been published.
Microsoft [34] ***Bulletin has been revised*[35]**	**Windows 95/98/ME/ NT 4.0/2000**	**Internet Explorer 5.0.1SP1&2, 5.5, 5.5SP1&2, 6.0**	**Two vulnerabilities exist: a vulnerability exists in the zone determination function, which could let a malicious user execute arbitrary script code; and vulnerability exists in the handling of object tags which could let a malicious user invoke an executable already present on the user's system.** ***Bulletin has been updated to clarify that patch does not contain MS02-009.***	**Frequently asked questions regarding these vulnerabilities and the patch can be found at:** **http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms02-015.asp**	**Internet Explorer Known Local File Script Execution** **CVE Names: CAN-2002-0077, CAN-2002-0078**	**Medium High** **(High if arbitrary code can be executed)**	**Bug discussed in newsgroups and websites.** **Vulnerability has appeared in the press and other public media.**

[31] Bugtraq, April 16, 2002.
[32] Bugtraq, April 8, 2002.
[33] Thor Larholm Security Advisory, TL#002, April 16, 2002.
[34] Microsoft Security Bulletin, MS02-015, March 28, 2002.
[35] Microsoft Security Bulletin, MS02-015 V1.1, April 8, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[36]	Windows 98/ME/NT 4.0/2000	Internet Explorer 6.0	A vulnerability exists when the 'back' button is used to navigate to a JavaScript: URL, which could let a malicious user inject arbitrary JavaScript code in the browser history list and execute it.	No workaround or patch available at time of publishing.	Internet Explorer History List	**High**	Bug discussed in newsgroups and websites. Exploit script has been published. Vulnerability has appeared in the press and other public media.
Microsoft[37]	Windows 98/ME/NT 4.0/2000	Internet Explorer 6.0	A Denial of Service vulnerability exists when an URL is accessed that contains an excessive number of Unicode characters.	No workaround or patch available at time of publishing.	Internet Explorer Unicode Character Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft[38]	Office 2000, XP	Office Web Components (OWC) 9, 10	A vulnerability exists in the 'Paste' method of the 'Range' object and the 'Copy' method of the 'Cell' object, which could let a malicious user gain control over the clipboard even when the 'Allow paste operations via script' security feature in IE is disabled.	No workaround or patch available at time of publishing.	Office Web Component Clipboard Information Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft[39]	Windows 2000, XP	Office Web Components (OWC) 9, 10	A vulnerability exists in the 'LoadText' method of the Range object, which could let a malicious user read the content of any known local file.	No workaround or patch available at time of publishing.	Office Web Component Local File	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[36] Bugtraq, April 14, 2002.
[37] Securiteam, April 16, 2002.
[38] GreyMagic Security Advisory, GM#007-IE, April 8, 2002.
[39] GreyMagic Security Advisory, GM#006-IE, April 8, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[40]	MacOS 7.0/8.0/9.0, MacOS X 10.x	Internet Explorer Macintosh Edition 5.1; Office 2001 For Macintosh SR1, Office 2001 For Macintosh, Office v. X; Outlook Express for MacOS 5.0-5.0.3; PowerPoint 98 for Mac; Excel v. X for Macintosh, 2001 for Macintosh; Entourage v. X for Macintosh, 2001 for Macintosh	Two vulnerabilities exist: a buffer over vulnerability exists because input to a certain HTML feature is not correctly handled, which could let a malicious user execute arbitrary code; and a vulnerability exists that can allow local AppleScripts to be invoked by a web page without automatically first calling the Helper application.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/ms02-019.asp *Note: Patches for PowerPoint 98 have not yet been released.*	Multiple Microsoft Products for MacOS File Vulnerabilities CVE Names: CAN-2002-0152, CAN-2002-0153	**High**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Microsoft[41]	Windows 2000, XP	Office Web Components (OWC) 9, 10	Numerous vulnerabilities exist: a vulnerability exists in the Chart component because the 'Load' method does not perform security checks on the assigned URL, which could let a malicious user obtain sensitive information; a vulnerability exists in the Spreadsheet component in OWC10 because the 'XMLURL' property blindly follows redirections, which could let a malicious user obtain sensitive information; and a vulnerability exists in the DataSourceControl component in OWC10 because the 'ConnectionFile' property does not perform security checks on the assigned URL, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Office Web Components Multiple Vulnerabilities	Medium	Bug discussed in newsgroups and websites. Exploits have been published. Vulnerabilities have appeared in the press and other public media.

[40] Microsoft Security Bulletin, MS02-019, April 16, 2002.
[41] GreyMagic Security Advisory, GM#008-IE, April 8, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[42]	Windows XP	Office Web Components 10	A vulnerability exists in the spreadsheet component when the 'setTimeout' method of the window object is used through the '=HOST()' formula, which could let a malicious user execute arbitrary script code even when Active Scripting has been disabled.	No workaround or patch available at time of publishing.	Office Web Components Active Script Execution	**High**	Bug discussed in newsgroups and websites. Exploit has been published. Vulnerability has appeared in the press and other public media.
Microsoft[43]	Windows NT 4.0/2000	SQL Server 7.0, 2000	Several of the Microsoft provided extended stored procedures fail to perform input validation correctly and are susceptible to buffer overruns, which could let a malicious user cause a Denial of Service or execute arbitrary code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-020.asp	SQL Server Buffer Overflow CVE Name: CAN-2002-0154	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Microsoft[44]	Windows 2000	Windows 2000 Advanced Server, 2000 Advanced Server SP1&2, 2000 Professional, 2000 Professional SP1&2, 2000 Server, 2000 Server SP1&2	A Denial of Service vulnerability exists when malformed data is submitted to port 445.	Workaround available at: http://support.microsoft.com/default.aspx?scid=kb;en-us;Q320751	Windows 2000 Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required. Vulnerability has appeared in the press and other public media.
Microsoft[45] ***Microsoft releases revised bulletin[46]***	**Windows NT 4.0/2000, XP**	**Windows 2000 Server, 2000 Advanced Server, 2000 Datacenter Server**	**A vulnerability exists because it is possible to lock Group Policy files, which could let a malicious user block the application of Group Policy within a Windows 2000 domain.** ***This patch supersedes the one provided in Microsoft Security Bulletin MS01-036.***	**Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-016.asp**	**Windows Group Policy File Block Policy** **CVE Name: CAN-2002-0051**	**Medium**	**Bug discussed in newsgroups and websites. There is no exploit code required.** ***Vulnerability has appeared in the press and other public media.***

[42] GreyMagic Security Advisory, GM#005-IE, April 8, 2002.
[43] Microsoft Security Bulletin, MS02-020, April 17, 2002.
[44] KPMG-2002011, April 17, 2002.
[45] Microsoft Security Bulletin, MS02-016, April 4, 2002.
[46] Microsoft Security Bulletin, MS02-016, April 8, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[47]	Windows 2000	Windows 2000 Terminal Services, 2000SP1&2	A security vulnerability exists because the Group Policies (GPO) will not be applied to users if the current number of connections to the GPO hosting server exceeds the number of installed user licenses, which could let a remote malicious user obtain unauthorized access and elevated privileges.	No workaround or patch available at time of publishing.	Windows Terminal Server Group Policy Bypass	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Microsoft [48] ***Microsoft updates bulletin***[49]	**Windows NT 4.0/2000, XP**	**Windows NT 4.0 Workstation, 4.0 Server, 4.0 Server, Enterprise Edition, Terminal Server Edition, 2000 Professional, 2000 Server, 2000 Advanced Server, XP Professional**	**A buffer overflow vulnerability exists due to improper input checking in the Multiple UNC Provider, which could let a malicious user gain complete over the machine.** ***Bulletin updated to clarify that Windows XP Home Edition is also affected.***	**Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-017.asp**	**Windows Multiple UNC Provider Buffer Overflow** **CVE Name: CAN-2002-0151**	**High**	**Bug discussed in newsgroups and websites.**

[47] Securiteam, April 10, 2002.
[48] Microsoft Security Bulletin, MS02-017, April 4, 2002.
[49] Microsoft Security Bulletin, MS02-017 V1.1, April 16, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[50, 51]	Windows NT 4.0/2000, XP	Microsoft IIS 4.0, 5.0, 5.1; Cisco Building Broadband Service Manager 4.x, 5.x, Call Manager 3.0-3.2, Unity Server 2.0-2.4	Multiple vulnerabilities exist: Buffer overrun vulnerabilities exist in the HTR ISAPI extension, one that involves the 'chunked encoding transfer mechanism' related to Active Server Pages, one that involves the interpretation of HTTP header delimiter information, and one that is related to the processing of requested filenames that are to be included in file includes in ASP scripts, which could let a remote malicious user execute arbitrary code; a Denial of Service vulnerability exists due to the way error conditions are handled from ISAPI filters and a Denial of Service vulnerability involving the way the FTP service handles a request for the status of the current FTP session; and several Cross-Site Scripting vulnerabilities exist: one involving the results page that's returned when searching the Help Files, one involving HTTP error pages; and one involving the error message that's returned to advise that a requested URL has been redirected, which could let a malicious user execute arbitrary script code. ***Note:*** *This vulnerability affects Cisco products and applications that are installed on Microsoft operating systems incorporating the use of the Internet Information Server.*	Frequently asked questions regarding these vulnerabilities and the patches can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-018.asp Users of Cisco Unity products and Cisco Building Broadband Service Manager 4.x/5.x are advised to apply Microsoft's cumulative patch. *Note: The fixes for four vulnerabilities affecting IIS 4.0 servers and vulnerabilities involving non-IIS products are not included in the patch. For more information, see Caveat Section in bulletin located at:* http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-018.asp.	Microsoft IIS Multiple Vulnerabilities CVE Names: CAN-2002-0071, CAN-2002-0072, CAN-2002-0073, CAN-2002-0074, CAN-2002-0075, CAN-2002-0079, CAN-2002-0147, CAN-2002-0148, CAN-2002-0149, CAN-2002-0150	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published for the Chunked Encoding Transfer Mechanism vulnerability. Exploit has been published for the HTTP Error Page Cross-Site Scripting Vulnerability. Vulnerabilities have appeared in the press and other public media.
Mirabilis[52]	Windows 95/98/ME/ NT 4.0/2000, XP	ICQ 2002 a Build#3722	A Denial of Service vulnerability exists when a user attempts to access a malformed .hpf file.	No workaround or patch available at time of publishing.	Mirabilis ICQ .hpf Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.

[50] Microsoft Security Bulletin, MS02-018 V1.2, April 12, 2002.
[51] Cisco Advisory, CI-02.04, April 15, 2002.
[52] Bugtraq, April 14, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[53]	Windows 95/98/ME/ NT 4.0/2000	BindView NETrc 1.0, 3.06; Funk Software Proxy 3.0, 3.06, 3.09, 3.09a,	Multiple vulnerabilities exist: a vulnerability exists because the default Proxy installation permissions are weak; a vulnerability exists because the Proxy Host password are stored in a recoverable format; and a vulnerability exists because the Proxy Host password can be obtained and configuration parameters arbitrarily changed by a remote malicious user. All of these vulnerabilities could allow unauthorized remote control access to the Windows GUI, which could be used to further compromise the system.	Workaround available at: http://razor.bindview.com/publish/advisories/adv_FunkProxy.html	Funk Software Proxy Multiple Vulnerabilities CVE Names: CAN-2002-0064, CAN-2002-0065, CAN-2002-0066	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Nortel Networks[54]	Multiple	CVX 1800 Multiservice Access Switch 3.6.3 p5, 3.6.3 p24	A vulnerability exists because a default SNMP community string of 'public' is contained in the device, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	CVX 1800 Multi-Service Access Switch Default SNMP Community	Medium	Bug discussed in newsgroups and websites. Vulnerability may be exploited with a SNMP client.
OpenBSD[55]	Unix	OpenBSD 2.9, 3.0	A vulnerability exists because the /usr/bin/mail program accepts escaped characters, which could let a malicious user embed arbitrary commands and obtain superuser privileges	Upgrade available at: http://www.openbsd.org/cgi-bin/cvsweb/src/usr.bin/mail/collect.c.diff?r1=1.23&r2=1.24	OpenBSD Root Compromise	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Oracle Corporation[56]	Multiple	Oracle9i 9.0, 9.0.1	A security vulnerability exists in the implementation of the ANSI 'outer join' syntax feature, which could let a malicious user bypass database access controls and obtain sensitive information.	Patch available at: http://isupport.oracle.com	Oracle 9i ANSI Outer Join Access Control Bypass	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Paul Kulchenko[57]	Unix	SOAP::Lite	A vulnerability exists when a qualified method is provided to the SOAP (Simple Object Access Protocol) call including Perl package names, which could let a malicious user execute arbitrary shell commands.	A vendor supplied patch should be available in the next version, although a release date is not yet available.	SOAP::Lite Remote Arbitrary Command Execution	**High**	Bug discussed in newsgroups and websites.

[53] BindView Security Advisory, April 8, 2002.
[54] Bugtraq, April 12, 2002.
[55] Bugtraq, April 11, 2002.
[56] SecurityFocus, April 16, 2002.
[57] SecurityFocus, April 11, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Power boards[58]	Multiple	Powerboards 2.2 b	Multiple vulnerabilities exist: a vulnerability exists because cookies are used for authentication and saved in an unencrypted format, which could let a malicious user obtain unauthorized access to admin resources; a vulnerability exists because no access restrictions to the posting capability exist, which could let an unauthorized malicious user delete entries; a vulnerability exists when a specially crafted request is submitted via the administrative script, which could let a malicious user obtain elevated privileges; a Cross-Site Scripting vulnerability exists because user-supplied input is not properly filtered, which could let a malicious user execute arbitrary script code; a vulnerability exists because when a user signs up to the service a file is created with the chosen username as the filename which could let a remote malicious user obtain sensitive information and potentially execute arbitrary code; and a vulnerability exists in the 'profiles.php' script, which could let a remote malicious user obtain the full path to the backend database.	No workaround or patch available at time of publishing.	Powerboards Multiple Vulnerabilities	Medium/ **High** **(High if administrative access can be obtained or if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
PVote[59]	Multiple	PVote 1.0, 1.0.a, 1.0 b, 1.5	Multiple vulnerabilities exist because a lot of the scripts in the PVote package do not properly validate the user and a vulnerability exists that lets anyone change the Admin password, which could let a remote malicious user obtain elevated privileges and add/delete information.	Upgrade available at: http://orbit-net.net:8001/php/pvote/pvote.zip	PVote Multiple Vulnerabilities	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.

[58] SecurityFocus, April 9, 2002.

[59] Telhack Security Advisory - #1, April 18, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Sambar Technologies[60]	Widows 95/98/ME/ NT 4.0/2000	Sambar Server 5.1	A vulnerability exists in the severside URL parsing, which could let a malicious user obtain sensitive information or cause a Denial of Service..	Patch available at: http://sambar.dnsaloas.org/win32-preview.tar.gz	Sambar Server Script Source Disclosure	Low Medium (Medium if sensitive information is obtained)	Bug discussed in newsgroups and websites. Proof of concept exploit has been published.
SGI[61]	Unix	IRIX 6.5-6.5.10, 6.5.11m-6.5.15m, 6.5.11f-6.5.15f	Multiple vulnerabilities exist: a vulnerability exists in the 'mailx' and 'Mail' account utilities, which could let a malicious user obtain elevated privileges; a vulnerability exists in the 'sort' utility due to the usage of predictably-named temporary files; a vulnerability exists in the 'timed' utility which could cause a Denial of Service; and a buffer overflow vulnerability exists in the 'gzip' routine, which could let a malicious user obtain elevated privileges.	Patch available at: ftp://patches.sgi.com/support/free/security/patches/	SGI IRIX Mail Vulnerabilities	Medium	Bug discussed in newsgroups and websites.
SGI[62]	Unix	IRIX 6.5-6.5.9, 6.5.10&11m 6.5.10&11f	A Denial of Service vulnerability exists in the XFS filesystem if a local user creates a malicious file.	Patch available at: ftp://patches.sgi.com/	IRIX XFS Filesystem Denial of Service CVE Name: CAN-2002-0042	Low	Bug discussed in newsgroups and websites.
SSH Communications Security[63]	Unix	SSH for UNIX 1.2.33, SSH2 3.0, 3.0.1	A vulnerability exists which could let a remote malicious user upload files to world-writeable directories, and execute commands from world-writeable directories.	No workaround or patch available at time of publishing.	SSH Restricted Shell Escaping Command Execution	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
StepWeb[64]	Unix	SWS 2.5	A vulnerability exists because password credentials for administrative scripts are hardcoded links on the admin page, which could let a remote malicious user obtain access to administrative functions.	No workaround or patch available at time of publishing.	StepWeb Search Engine Administrative Access	**High**	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.

[60] KPMG-2002012, April 18, 2002.
[61] SGI Security Advisory, 20020401-01-P, April 10, 2002.
[62] SGI Security Advisory, 20020402-01-P, April 15, 2002.
[63] Bugtraq, April 18, 2002.
[64] Securiteam, April 14, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Symantec[65]	Unix	Enterprise Firewall 7.0 Solaris, Raptor Firewall 6.5.3 Solaris	A vulnerability exists because the software is prone to FTP bounce attacks, even if the FTP server in the network it protects is not vulnerable to such attacks, which could let a malicious user cause the FTP server to make a connection to an arbitrary host.	Patches available at: ftp://ftp.symantec.com/public/updates/ftpd-653-3des.tar and ftp://ftp.symantec.com/public/updates/ftpd-70s-3des.tar	Raptor / Enterprise Firewall for Solaris FTP Bounce	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Symantec[66]	Multiple	Norton Personal Firewall 2002	A vulnerability exists due to the way portscans are handled, which could let a malicious user bypass protscan protection.	No workaround or patch available at time of publishing.	Norton Personal Firewall 2002 Portscan Protection Bypass	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Symantec[67]	Multiple	Norton Personal Firewall 2002	A Denial of Service vulnerability exists because packet fragments are not properly filtered.	No workaround or patch available at time of publishing.	Norton Personal Firewall 2002 Denial of Service	Low/**High** **(High if DDoS best practices not in place)**	Bug discussed in newsgroups and websites.
TalentSoft[68]	Windows 95/98/NT 4.0/2000, Unix	Web+ Server 5.0	A buffer overflow vulnerability exists when a WML file is requested and an overly long cookie is supplied, which could let a malicious user execute arbitrary code as SYSTEM.	Patch available at: http://www.talentsoft.com/download/download.en.wml	Web+ WML Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Tarantella[69]	Unix	Enterprise 3 3.10, 3.11, 3.20	A vulnerability exists in the 'install.cgi' script because some configurations are not correctly handled, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Enterprise 3 Install.CGI Sensitive Information	Medium	Bug discussed in newsgroups and websites.
Turnkey WebTools[70]	Multiple	SunShop Shopping Cart 1.5, 2.0-2.2, 2.4-2.5	A Cross-Site Scripting vulnerability exists because user input is not checked for malicious code, which could let a remote malicious user obtain administrative access and execute arbitrary code.	Upgrade available at: http://www.turnkeywebtools.com/products.php?product=sunshop	SunShop Shopping Cart Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Proof of concept exploit has been published.

[65] Bugtraq, April 15, 2002.
[66] Bugtraq, April 16, 2002.
[67] Bugtraq, April 16, 2002.
[68] NGSSoftware Insight Security Research Advisory, NISR17042002B, April 17, 2002.
[69] SecurityFocus, April 9, 2002.
[70] Bugtraq, April 15, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Watch Guard[71]	Multiple	SOHO Firewall 5.0.35	A vulnerability exists when IP restrictions are configured on certain IP addresses, which could let a remote malicious user obtain unauthorized access to a allegedly secure network.	Upgrade available at: https://www3.watchguard.com/archive/login.asp	SOHO Firewall IP Restrictions	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Watch-guard[72]	Multiple	SOHO Firewall prior to 5.0.35	A Denial of Service vulnerability exists when a malicious user sends TCP traffic that contains malformed IP options through the firewall.	Upgrade available at: http://www.watchguard.com	SOHO Firewall Denial of Service	Low/**High** **(High if DDoS best practices not in place)**	Bug discussed in newsgroups and websites.
WebTrends[73]	Windows NT 4.0/2000	Reporting Center for Windows 4.0 d	A buffer overflow vulnerability exists when an oversized GET request is submitted, which could let a malicious user execute arbitrary code with SYSTEM privileges.	No workaround or patch available at time of publishing.	Reporting Center Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Proof of concept exploit has been published.
Woltlab[74]	Multiple	Burning Board 1.1.1	A vulnerability exists because a malicious user can create a link that is capable of causing malicious actions to be performed on behalf of a legitimate user.	No workaround or patch available at time of publishing.	Burning Board URL Parameter Manipulation	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
x-dev[75]	Multiple	xNewsletter 1.0	A vulnerability exists because form field input is not sanitized, which could let a malicious user execute arbitrary code.	Administrators should contact the vendor about obtaining a fix.	xNewsletter Form Field Input Validation	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

*"Risk" is defined by CyberNotes in the following manner:

High - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.

Medium – A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.

Low - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. *DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.*

[71] KPMG-2002008, April 10, 2002.
[72] KPMG-2002007, April 8, 2002.
[73] NGSSoftware Insight Security Research Advisory, NISR17042002C, April 17, 2002.
[74] Bugtraq, April 13, 2002.
[75] ITCP Advisory 12, April 14, 2002.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between April 8 and April 16, 2002, listed by date of script, script names, script description, and comments. **Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing**. During this period, 7 scripts, programs, and net-news messages containing holes or exploits were identified. *Note: At times, scripts/techniques may contain names or content that may be considered offensive.*

Date of Script (Reverse Chronological Order)	Script Name	Script Description
April 16, 2002	Centurion.tar.gz	Centurion checks any CGI script on a remote server for vulnerabilities such as directory traversal bugs, null byte, and incorrect filtering of metacharacters.
April 16, 2002	Linspy2beta2.tgz	Keystroke logger for Linux kernels v2.2 and 2.4 that records TTY activity.
April 15, 2002	Obsd-cron.c	Script which exploits the OpenBSD Root Compromise vulnerability.
April 15, 2002	Wellenreiter-v10.tar.gz	A GTK/Perl program that makes the discovery and the auditing of 802.11b wireless-networks much easier. It has an embedded statistics engine for the common parameters provided by the wireless drivers, enabling you to view details about the consistency and signal strength of the network. A scanner window can be used to discover access-points, networks, and ad-hoc cards.
April 14, 2002	**Ie_history.html**	**Exploit for the Internet Explorer History List vulnerability.**
April 11, 2002	**Innexpl.tar.gz**	**Script which exploits the InterNetNews Multiple Vulnerabilities.**
April 8, 2002	Lcrzoex-4.08-src.tgz	A toolbox for network administrators and network malicious users that contains over 200 functionalities using network library lcrzo.

Trends

- **A new Version of the "Klez" I-Worm is spreading fast. For more information, see Virus Section.**
- **The Computer Emergency Response Team (Cert) has released a report pinpointing the six fastest evolving trends in the black hat world of Internet security. The most notable trend to evolve over recent years is the automation and speed of attack tools. The full report can be found at: http://www.cert.org/archive/pdf/attack_trends.pdf.**
- **Windows users should be suspicious of a new Internet worm that is disguised as a Microsoft security bulletin. The "W32/Gibe" worm masquerades as an "Internet Security Update" from Microsoft Corporation.**
- **The CERT/CC has received reports of social engineering attacks on users of Internet Relay Chat (IRC) and Instant Messaging (IM) services. Intruders trick unsuspecting users into downloading and executing malicious software, which allows the intruders to use the systems as attack platforms for launching distributed denial-of-service (DDoS) attacks. The reports to the CERT/CC indicate that tens of thousands of systems have recently been compromised in this manner. For more information, see CERT® Incident Note IN-2002-03, located at: http://www.cert.org/incident_notes/IN-2002-03.html.**

Viruses

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication**. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available**. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported during the latest three months), and approximate date first found. During this month, a number of anti-virus vendors have included information on Trojan Horses and Worms. Following this table are descriptions of new viruses and updated versions discovered in the last two weeks. NOTE: At times, viruses may contain names or content that may be considered offensive.

Ranking	Common Name	Type of Code	Trends	Date
1	W32/SirCam	Worm	Stable	July 2001
2	W32/BadTrans	Worm	Stable	April 2001
3	W32/Nimda	File, Worm	Slight Increase	September 2001
4	W32/Klez	Worm	Slight Decrease	January 2002
5	W32/Hybris	File, Worm	Stable	November 2000
6	W32/Magistr	File, Worm	Stable	March 2001
7	Funlove	File	Stable	November 1999
8	FBound	Worm	Stable	March 2002
9	MyLife	Worm	New to Table	April 2002
10	Apology (MTX)	File Infector, Trojan	Return to Table	September 2000

Note: Virus reporting may be weeks behind the first discovery of infection. A total of **203** distinct viruses are currently considered "in the wild" by anti-virus experts, with another **409** viruses suspected. "In the wild" viruses have been reported to anti-virus vendors by their clients and have infected user machines. The additional suspected number is derived from reports by a single source.

ABAP_RIVPAS.A (Aliases: SAPVirii, WILLIE.A, RIVPAS.A): This proof of concept virus infects SAP R/3 programs and reports. Upon execution, this virus, which is written in Advanced Business Application Programming Language (ABAP), attempts to find the SAP report directory in the system, where it searches for functions and reports to infect. The virus routine checks for the virus signature on the file it is about to infect. The infection marker is as follows: SAPVirii.

HTML.Redlof.A: This is a polymorphic, encrypted Visual Basic script virus that infects .html and .htt files on all drives. When HTML.Redlof.A is run, the virus decrypts its viral body and executes it. The virus searches for files that have the file extensions .html and .htt in all folders on all drives and infects those files.

O97M.Toraja.G (Office 97 Macro Virus): This is a variant of Toraja. It infects Microsoft Excel and Microsoft Word files. O97M.Toraja.G infects Word documents by infecting Normal.dot and the dropped file, C:\Autostart01.dot. It infects Excel workbooks by dropping the file AutoStart01.xls in the \XLStart folder. All of the AutoStart files dropped by this macro are read-only files. Viral code is imported and exported using C:\Autostart01.dat, which is a hidden file. When the infected templates or startup files are in place, O97M.Toraja.G infects documents or workbooks when they are created. It creates or infects templates and startup files when infected files are closed. It autosaves upon infection.

PE_ELKERN.D (Alias: ELKERN.D) (File Infector Virus): This encrypted, per-process, memory-resident file infector infects PE files (Windows executables). It is a cavity-type virus that inserts itself in the unused spaces of the target file. When there is no free space remaining, it appends its code at the end of the file.

PE_MOE.A (Alias: MOE.A) (File Infector Virus): This polymorphic, mass-mailing worm propagates via Microsoft Outlook. It infects *.exe and *.scr files and drops a copy of itself in the Windows directory.

VBS/Chick-C (Aliases: I-Worm.Brit.c, VBS.Chick.C@mm) (Visual Basic Script Worm): This worm is similar to VBS/Britney-A. It spreads via both Microsoft Outlook and IRC networks. The worm copies itself to "SHAKIRA.CHM" in the Windows folder and then e-mails itself to the first address in the Outlook address list. The e-mail contains the attachment, "SHAKIRA.CHM." The worm requires ActiveX to be enabled for the VBScript to run and prompts the user to enable ActiveX with the message "Permite Active X para ver el nuevo video de SHAKIRA." VBS/Chick-A searches drives C:, D:, and E: for the presence of a file called "MIRC.INI." If it finds this file, then the worm creates a SCRIPT.INI file, which will then attempt to send copies of the files to other IRC users.

VBS_PINOCC.A (Alias: PINOCC.A) (Visual Basic Script Malware): This Visual Basic Script malware uses Messaging Application Programming Interface (MAPI) to propagates copies of itself via e-mail. It overwrites the "SCRIPT.INI" of an infected system so that it can also propagate via Internet Relay Chat (mIRC).

VBS.Resreg@mm (Visual Basic Script Worm): This is an Internet worm that is written in VBScript. It uses Microsoft Outlook to spread as the attachment "Freemp3s.vbs." If the attachment is run, it does the following: It copies itself to the root of drive C as "Freemp3s.vbs." Next it uses Microsoft Outlook to send itself to the first 101 recipients in the address book. It then deletes "Freemp3s.vbs." VBS.Resreg@mm has a type of "backup and recovery" mechanism that it can use to reinstall itself. The script writes 4695 bytes, the hex equivalent of "Freemp3s.vbs," into a registry key that it creates:

HKEY_LOCAL_MACHINE\Alcopaul

The worm also creates the VBScript decoder file, "Excel.vbs." It modifies the registry so that "Excel.vbs" is executed if any other .vbs file is executed. It does this by changing the Value Data of the (Default) value from "%1" /S to "wscript.exe c:\excel.vbs" in the registry key:

HKEY_CLASSES_ROOT\scrfile\shell\open\command\

When Excel.vbs is run, it recreates the mass-mailing script by reading the data from the Alcopaul registry key, writes a script as C:\Registry.vbs, executes the script, and then deletes the Registry.vbs file.

W32/Aplore-A (Win32 Worm): This is a Win32 worm that uses Microsoft Outlook to spread. It copies itself into the Windows system directory as "explorer.exe" and "psecure20x-cgi-install6.01.bin.hx.com" and adds the following value to the registry to run itself on Windows startup:

HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Explorer = "<windows system folder>\explorer.exe"

When run, the worm drops and runs the VBScript, "e-mail.vbs," which attempts to send an e-mail with the worm files attached to all contacts from the Outlook address book. The e-mails contains the attached file, '"psecure20x-cgi-install.version6.01.bin.hx.com." W32/Aplore-A also contains an IRC client and an HTTP server. Before the internal web server is started, the worm drops the file "index.html" that acts as a homepage for the server. When the server is started, it listens for a connection on port 8180. The IRC client attempts to connect to an IRC server and join several channels with a nickname randomly chosen from a list of female names stored in the worm code. The worm sends messages containing a link to the infected machine's web server to the IRC channels. The messages sent to the IRC channel contain the text "FREE PORN:" and the IP address of the infected machine. If a user attempts to connect to the server, then the server sends the previously dropped index.html.

W32/Dander.worm (Win32 Worm): This is a worm designed for the Spanish version of Windows. When run, it displays a fake error message. The worm copies itself to the Spanish Windows Start Up group, C:\windows\Menú inicio\programas\inicio\WinX32.exe. It remains resident in memory and copies itself to the A:\ drive every minute.

W32/ElKern-C (Alias: W32.Elkern.4926) (Win32 Virus): This is an executable file virus very similar to W32/ElKern-A. W32/ElKern-C works under Windows 98, Windows ME, Windows 2000, and Windows XP. It is capable of infecting file cavities, meaning that it may not change the size of files it infects. The virus is dropped into the Program Files folder and run by W32/Klez-H. W32/ElKern-C contains routines to disable the on-access component of virus scanners developed by major anti-virus software vendors. The body of the virus contains the text "Win32 Foroux V1.0" in an encrypted format.

W32/Hunch-C (Win32 Worm): This is an e-mail worm that uses Microsoft Outlook to spread. It arrives in an e-mail with the body text:

> "Tal como te prometí; te envío mi foto en el archivo adjunto..."

The subject and attachment name are dependent on the original filename. When the worm runs it copies itself to:

> C:\Windows\System\Thd16.exe
> C:\Windows\System\Msoffice.exe
> C:\Windows\System\<attachment filename>

and adds the registry value:

> HKLM\Software\Microsoft\Windows\CurrentVersion\Run\THD16 =
> C:\Windows\System\Thd16.exe

so the worm runs on startup. The worm will delete up to five files and records the names of the files it deletes in C:\Windows\System\ListWin.txt. Finally the worm displays a pornographic image.

W32/MyLife-G (Win32 Worm): This is a Win32 worm that copies itself to the Windows system directory as "ox&Wife.scr" and sets the following registry value to run the copy on restart:

> HKCU\Software\Microsoft\Windows\CurrentVersion\Run\OX

When first executed, the worm will check to see if the file "ox&Wife.scr" exists in the system directory. If the file does exist, then a message box will be displayed with the title "KiLlLlLl aNd KiLlLlLl" and the message text "KiLlLlLl sHaRoN bY: mY lIfE 1-oVeR wRiTe 30 <==> eXtEnSiOn 2-dElEte aLl fOlDeRs (C to I) 3-LoOOoOOoL." The worm will then attempt to delete the contents of drives C: to I:. If the copy of the worm does not exist, a window will be displayed with the title "SHARON," containing a caricature of an ox along with the text "wE*sAy*iT's*oX*tHeY*sAy*mIlK*iT*!!." The worm then sends itself to addresses from the Outlook address book, using an e-mail with the attached file, "ox&Wife.scr."

W32/MyLife-H (Win32 Worm): This is a Win32 worm which arrives in an e-mail with the following characteristics:

> Subject line: peeeeeep
> Attached file: peeeeep.mpeg.scr

If the user runs the attachment, the worm saves a copy of itself in the root folder then sends itself to addresses from the Outlook address book and MSN Messenger contact list. The worm will send itself everytime it is executed. The worm also attempts to send a list of addresses used in an e-mail with the following characteristics:

> To: asdsdfd315@hotmail.com
> Subject line: new

W32.Mylife.I@mm (Aliases: MYLIFE.I, WORM_MYLIFE.I) (Win32 Worm): This UPX-compressed mass-mailing worm uses Microsoft Outlook to send itself to all users listed in the infected user's address book. The e-mail arrives with the subject line "peeeeep picture" and the attachment "peeeep~~~.scr," which carries the worm.

W32/MyLife-J (Win32 Worm): This is a Win32 worm that copies itself to the Windows system folder as "usa.scr" and "sh.scr." It creates the following registry value so that the copy will be run on Windows startup:

HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Scr

When first executed, the worm will check to see if the file "usa.scr" exists in the system directory. If the file does exist and the time is between 9 a.m. and 10 a.m., the worm will delete all files from drive C:. If the copy of the worm does not exist, then a window will be displayed with the title "SHARON," containing a caricature of an ox along with the text "wE * sAy *iT's* oX * tHeY * sAy * mIlK * iT * !!." The worm then sends itself to addresses from the Outlook address book, using an e-mail with the attached file, "usa.scr."

W32/Onamu@MM (Win32 Virus): This mass-mailing worm sends itself to addresses found in the Windows Address book, and addresses harvested from cached webpages. It also infected executable files on the local system. When run, a message box is displayed. A copy of the virus is saved to the Windows directory with a random five-character name and an .EXE extension. A registry run key is created to load the virus at startup.

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\
Run\%FileName_without_extension%=%VirusPath%

The worm sends itself to everyone in the Windows Address Book and MAILTO: addresses found in *.HT* files on the hard disk using SMTP. The default SMTP server is retrieved from the Internet Account Manager registry setting:

HKEY_CURRENT_USER\Software\Microsoft\Internet Account Manager

There are 20 possible e-mail messages sent out by the worm. The file infection routine infects .EXE and .SCR files in the WINDOWS directory and subdirectories.

W32/Pimaf@MM (Win32 Virus): This e-mail worm, written in Microsoft Visual C++, is packaged with a SMTP function library (used for Base64 encoding) using PEBundle. The worm carries its own SMTP engine for mailing. When executed on the victim machine, the worm checks for the existence of a crudely named text file in C:\Windows. If the file does not exist, a message is displayed. The worm extracts e-mail addresses from within the Outlook Express 'Sent-Items' folder (stored on disk within the SENT ITEMS.DBX). If replicated successfully, the e-mail message contents are:

Attachment: MyNewPics.PIF
Body: Hi I finally got new pics of myself scanned in and put them in this Picture Image File (PIF)
Tell me what you think :-)

The worm attempts to trick the user into believing that the PIF file consists of merely images. It is in fact a standard Windows program information file. The worm also copies itself to the Windows folder, and sets the following Registry key to ensure its execution on subsequent system startup:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows_ CurrentVersion\Run "(crude string)" = C:\WINDOWS\MyNewPics.PIF

W32.Trilisa@mm (Win32 Worm): This is a worm that sends itself to all addresses in the Microsoft Outlook address book. It renames all files that are in the \Windows folder and that have the .exe or .scr file extension; the worm then copies itself as the original file name. It also deletes files that have specific file extensions, as well as the files Regedit and Regedb32.

W97M.Destrib (Word 97 Macro Virus): This is a Microsoft Word macro virus that infects documents when you open them. This virus exports and imports code using the Microsoft Word document Destrib.dll in the \Office folder.

WM97/Marker-KQ (Alias: W97M.Marker.KQ) (Word 97 Macro Virus): This virus has payloads which trigger on both opening and closing of infected documents. On opening an infected document between the 23rd and 31st of July, the virus displays the question, "Do you love mr occonor?." When an infected document is closed between the 23rd and 31st of July, the virus changes the application title to "bob oconnor certainly is gay and does practice brown love" and displays the question, "Did You shag mr occonnor?." If the user answers yes, the virus displays the message, "my god I knew you was gay." If the user answers no, the virus displays a message that starts " well you should." The virus also changes the properties of infected Word documents as follows:

Title: you love mr occonor?
Subject: STD'd
Author: you
Keywords: brown love
Comments: mr occonor still hangs outside your window at night.

WM97/Marker-KS (Word 97 Macro Virus): This is a corrupt but viable variant of the WM97/Marker-C virus. Whenever an infected document is closed, the virus attempts to FTP user information from Word to the Codebreakers site and appends this information to the bottom of the macro as comments.

WM97/Titch-L (Word 97 Macro Virus): This virus is a member of the WM97/Titch family that has no malicious payload. It creates the non-viral file C:\arbind2000.tmp, which it uses during replication. The virus will normally delete this file after use.

WORM_KELINO.A (Aliases: I-Worm.Kelino, KELINO.A) (Internet Worm): This worm propagates copies of itself via e-mail to all recipients listed in the infected user's Address Book. It also sends an e-mail to its author. The e-mail message contains information about the infected system.

WORM_KLEZ.G (Aliases: W32/Klez-G, I-Worm.Klez.h, I-Worm.W32/Klez.gen@MM, W32.Klez.H@mm) (Internet Worm): This worm has been reported in the wild. It is a memory-resident variant of the WORM_KLEZ.A mass-mailing worm that uses SMTP to propagate via e-mail. The subject line of the e-mail is randomly selected from a list of possible choices. Upon execution, this worm drops files and creates an entry in the AutoRun key of the system registry. This worm does not perform its Antivirus Retaliation routine on machines running NT 4.0 or lower, due to an unavailability of system functions or APIs it uses to kill the antivirus-related processes. It also carries a new version of the partially encrypted Elkern virus. This is capable of spreading through network drives and the new version may be capable of deleting files on a pre-determined date.

WORM_ORKIZ.A (Aliases: I-worm.orkiz, ORKIZ.A) (Internet Worm): This worm uses Messaging Application Programming Interface (MAPI) to propagate copies of itself via e-mail. It drops and then executes Visual basic script files that contain instructions to send an e-mail to all e-mail recipients listed in the infected user's address book. It copies all the EXE files in the Windows directory as EX_ files and then modifies the EXE files with its code.

X97M.Divi.O (Excel 97 Macro Virus): This is a standard Microsoft Excel macro virus. The virus replicates when a workbook is opened. When X97M.Divi.O is executed, it drops a copy of its viral code as the file \XLStart\ErisH.xls. This ensures that the virus is loaded whenever you start Excel.

X97M/Reten.d (Excel 97 Macro Virus): This virus can infect both Excel 97 and Excel 2000 workbooks. The virus exists in a macro module named "Project_P" and uses a dropper file in the XLSTART folder named "ValeriaNET.XLM." On opening the infected workbook Tools/Macro, Tools/Add-Ins and Tools/Customize command bars are disabled. A message is displayed in Indonesian on the Excel Application status bar. When the workbook is closed, the virus creates the text file C:\AlQuran.txt that contains an Indonesian messages. The caption for the Excel Application is changed to: "TELKOMSEL,Begitu Dekat Begitu Nyata...." The virus also creates Palestina.html and AsiaGirls.html that also contain Indonesian text. These files are not viral. On the 26th day of every month if time is after 10:26 a.m., the virus displays a message. If the day is equal to the minute Example: date 20/04/02 and time 13:20, another message is displayed.

Trojans

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table starts with Trojans discussed in CyberNotes #2002-01, and items will be added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks. Readers should contact their anti-virus vendors to obtain specific information on Trojans and Trojan variants that anti-virus software detects. *Note: At times, Trojans may contain names or content that may be considered offensive.*

Trojan	Version	CyberNotes Issue #
APStrojan.sl	N/A	CyberNotes-2002-03
Arial	**N/A**	**Current Issue**
Backdoor.EggHead	N/A	CyberNotes-2002-04
Backdoor.G_Door.Client	N/A	CyberNotes-2002-05
Backdoor.IISCrack.dll	N/A	CyberNotes-2002-04
Backdoor.NetDevil	N/A	CyberNotes-2002-04
Backdoor.Palukka	N/A	CyberNotes-2002-01
Backdoor.Subwoofer	N/A	CyberNotes-2002-04
Backdoor.Surgeon	N/A	CyberNotes-2002-04
Backdoor.Systsec	N/A	CyberNotes-2002-04
BackDoor-AAB	N/A	CyberNotes-2002-02
BackDoor-ABH	N/A	CyberNotes-2002-06
BackDoor-ABN	N/A	CyberNotes-2002-06
BackDoor-FB.svr.gen	N/A	CyberNotes-2002-03
BDS/Osiris:	N/A	CyberNotes-2002-06
BKDR_SMALLFEG.A	N/A	CyberNotes-2002-04
BKDR_WARHOME.A	N/A	CyberNotes-2002-06
Dewin	**N/A**	**Current Issue**
DlDer	N/A	CyberNotes-2002-01
DoS-Winlock	N/A	CyberNotes-2002-03
Downloader-W	**N/A**	**Current Issue**
Hacktool.IPStealer	N/A	CyberNotes-2002-02
Irc-Smallfeg	N/A	CyberNotes-2002-03
IRC-Smev	**N/A**	**Current Issue**
JS/Seeker-E	N/A	CyberNotes-2002-01
JS_EXCEPTION.GEN	N/A	CyberNotes-2002-01
mIRC/Gif	**N/A**	**Current Issue**
Multidropper-CX	**N/A**	**Current Issue**
SecHole.Trojan	N/A	CyberNotes-2002-01
Troj/Download-A	N/A	CyberNotes-2002-01
Troj/ICQBomb-A	N/A	CyberNotes-2002-05
Troj/Msstake-A	N/A	CyberNotes-2002-03
Troj/Optix-03-C	N/A	CyberNotes-2002-01
Troj/Sub7-21-I	N/A	CyberNotes-2002-01
Troj/WebDL-E	N/A	CyberNotes-2002-01
TROJ_CYN12.B	N/A	CyberNotes-2002-02

Trojan	Version	CyberNotes Issue #
TROJ_DANSCHL.A	N/A	CyberNotes-2002-01
TROJ_DSNX.A	N/A	CyberNotes-2002-03
TROJ_FRAG.CLI.A	N/A	CyberNotes-2002-02
TROJ_ICONLIB.A	N/A	CyberNotes-2002-03
TROJ_JUNTADOR.B	N/A	CyberNotes-2002-06
TROJ_SMALLFEG.DR	N/A	CyberNotes-2002-04
Trojan.Badcon	N/A	CyberNotes-2002-02
Trojan.StartPage	N/A	CyberNotes-2002-02
Trojan.Suffer	N/A	CyberNotes-2002-02
VBS.Gascript	N/A	CyberNotes-2002-04
VBS_CHICK.B	N/A	CyberNotes-2002-07
VBS_THEGAME.A	N/A	CyberNotes-2002-03
W32.Alerta.Trojan	N/A	CyberNotes-2002-05
W32.Delalot.B.Trojan	N/A	CyberNotes-2002-06
W32.Maldal.J	N/A	CyberNotes-2002-07

Arial: This Trojan is spread by telling you that you are infected and to go to some site for a cleaner. The other way is supposed to be joke pictures about Osama bin Laden. Both are hoaxes and if you go to these websites with an unpatched web browser, you may become automatically infected. If you use Netscape 6.x, you should update to version 6.2.2. All Netscape users, no matter which version should disable all Active-X and Java and Java settings in File | Preferences | Advanced.

Dewin (Alias: Backdoor.Dewin): This is a backdoor Trojan that can be used by a malicious user to install unwanted programs from a website to the victim machine. When started, it copies itself to the Windows Directory as 'Winreg.exe.' This copy of the file is added to the registry as:

'HKLM\Software\Microsoft\Windows\CurrentVersion\Run\SystemReg

Downloader-W: There are several components to this Trojan. They are:

- MNSVC.EXE (20480 bytes) - This is the part that downloads AUSVC.EXE from http://www.wwws1.com/. It contains the text: "MinStaller Mutex"
- AUSVC.EXE (57344 bytes) - This downloads the rest of the Trojan. It contains the text: "Autoupdater Mutex"
- BVT.EXE (114760 bytes) - This is an Internet Explorer Browser Plugin. It contains the text "BrowserEvt"
- ABSR.EXE (118858 bytes) - This is another IE Plugin. It contains the text "AutoBrowser"
- AUUPG.EXE (69632 bytes) - This appears similar to AUSVC.EXE, but it doesn't have the same text.

IRC-Smev: This IRC Trojan exploits various legitimate tools in order to infect the victim machine. The Trojan also acts as a worm, spreading itself to vulnerable machines on the network. A single batch file provides the basis for infection, running at mIRC client startup. The batch file performs the following tasks: A standard system utility is used to find vulnerable machines (queried by IP address). Assuming a vulnerable machine is found, network propagation proceeds, if not, a different remote machine is probed. A second script file is then called that attempts to connect to the 'C$' share on the remote machine considered vulnerable. This is attempted with the username 'Administrator,' and with usernames determined from the previous step. Next, a utility for running remote processes is used to copy two files onto this share and execute them:

- a self-extracting file archive, containing associated Trojan components and a mIRC client
- a batch file which copies the SFX contents to C:\WINNT\SYSTEM32\SH, adds the following Registry hook (to run the mIRC client - renamed to WIN32.EXE), runs the mIRC client, and then deletes itself.

HKEY_LOCAL_MACHINE\Software\Micrsoft\Windows_ CurrentVersion\Run
"Wins32" = C:\WINNT\SYSTEM32\SH\WIN32.EXE

Once running the Trojan will act as an IRC bot on the victim machine, attempting to connect to various IRC servers (listed within a text file contained within the SFX mentioned above). Once connected, the bot can receive various remote commands. For example:

- spawn network propagation routine
- die
- join channel
- clean (runs a batch file to remove temporary files)
- restart (restarts bot)
- remove bot from victim machine (run a batch file again)

mIRC/Gif: This is a Trojan that is programmed to spread through the popular chat application mIRC. This is not a particularly dangerous Trojan, as in order to spread the user must deliberately send it to other people connected to IRC. mIRC/Gif stands out for its capacity to disguise itself, it can disguise itself almost perfectly as a 'gif' file, as its malicious script (in other words, the Trojan's code) contains the header and extension of this type of graphics file.

Multidropper-CX: This Multidropper Trojan simply drops and runs two other Trojans:

- BackDoor-Sub7.svr (into the %Temp% and %System% folders)
- BackDoor-TW (into the %Temp% folder)